UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/970,051	10/21/2004	Richard F. Carrott	CAR.5000CONT	5569

60817 7590 05/02/2017

Frederick W. Gibb, III, Esq.
GIBB & RILEY, LLC
844 West Street
Suite 100
ANNAPOLIS, MD 21401

EXAMINER
KIM, STEVEN S

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
05/02/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

support@gibbiplaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte RICHARD F. CARROTT and HIRSHOL H. PHEIR

Appeal 2015-005953[1]
Application 10/970,051[2]
Technology Center 3600

Before MURRIEL E. CRAWFORD, MATTHEW S. MEYERS, and ALYSSA A. FINAMORE, *Administrative Patent Judges*.

FINAMORE, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134 from a rejection of claims 1, 5–10, 13–18, 21, and 23–30. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

---

[1] Our Decision considers Appellants' Appeal Brief ("Br.," filed Jan. 20, 2015), as well as the Examiner's Final Office Action ("Final Act.," mailed Aug. 21, 2014), Advisory Action ("Adv. Act.," mailed Oct. 28, 2014), and Answer ("Ans.," mailed Mar. 27, 2015).

[2] Appellants identify Benedor Corporation as the real party in interest. Br. 3.

CLAIMED SUBJECT MATTER

The claimed invention "generally relates to a system for providing security for purchase transactions made over a network and more particularly to an improved security system that only stores and provides encrypted information." Spec. 1:9–11. Claims 1, 10, and 18 are the independent claims on appeal. Claim 1, reproduced below, is illustrative of the claimed subject matter:

> 1. A method of securing transactions over a computer network comprising:
>
> encrypting customer information as a customer code on a storage device on a customer computer, said customer computer being connected to said computer network, said customer information comprising a customer address and a customer credit card number, said customer information being stored on said storage device only in encrypted form;
>
> requiring a computer system identifier of said customer computer, and one of a private key, a password, and a personal access code of a customer as an entry to said customer computer to access said customer code on said storage device of said customer computer;
>
> supplying said customer code to a merchant in a transaction over said computer network;
>
> forwarding said customer code to a financial institution over said computer network;
>
> decrypting said customer code at said financial institution; and
>
> returning an authorization decision from said financial institution to said merchant over said computer network.

REJECTIONS

Claims 1, 5–10, 13–17, 28, and 29 are rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.

Claims 1, 5–10, 13–17, 21, 23–26, 28, and 29 are rejected under 35 U.S.C. § 112, second paragraph, as indefinite.[3]

Claims 1, 5–10, 13–18, 21, and 23–30 are rejected under 35 U.S.C. § 103(a) as unpatentable over Flitcroft (US 2003/0028481 A1, pub. Feb. 6, 2003), Schenkler (US 6,078,902, iss. June 20, 2000), Shmueli (US 2002/0143637 A1, pub. Oct. 3, 2002), and Mi (US 6,418,472 B1, iss. July 9, 2002).

ANALYSIS

Written Description

The Examiner finds there is no written description support for the limitation reciting "requiring a computer system identifier of said customer computer, and one of a private key, a password, and a personal access code of a customer as an entry to said customer computer to access said customer code on said storage device of said customer computer" in each of independent claims 1 and 10. Final Act. 5–7; Adv. Act. 2; Ans. 3. Appellants argue that the disclosure on page 8, lines 11–17 of the

[3] The heading of the rejection omits independent claims 1 and 10 and dependent claims 5, 8, 9, 13, 17, 28, and 29. Final Act. 8. We consider the omission of these claims from the heading to be a typographical error because the body of the rejection discusses independent claims 1 and 10. *Id.* Appellants also acknowledge that independent claims 1 and 10 are subject to this rejection. Br. 9–10. Moreover, the heading of this rejection includes independent claim 18 and claims 22, 27, and 30 depending therefrom. Final Act. 8. Claim 22 has been canceled. Amendment filed Oct. 16, 2014. Further, the Examiner has withdrawn the rejection as to independent claim 18 (Ans. 5) and claim 27 (*id.* at 7), and the body of the rejection does not discuss claim 30. Accordingly, the rejection before us on appeal does not include these claims.

Specification provides sufficient support for the disputed limitation. Br. 8–9. Appellants' argument is not persuasive.

Although the cited portion of the Specification describes a customer's computer system identifier and the customer's private key are required to access the customer code, i.e., the encrypted information, we agree with the Examiner that there is no description of these pieces of information being required to enter the customer's computer. Final Act. 7; Adv. Act. 2; Ans. 3. As such, we sustain the rejection of independent claims 1 and 10 and dependent claims 5–9, 13–17, 28, and 29 under 35 U.S.C. § 112, first paragraph.

Indefiniteness

Independent claims 1 and 10 and dependent claims 5, 8, 9, 13, 17, 28, and 29

The Examiner determines the limitation reciting "requiring a computer system identifier of said customer computer, and one of a private key, a password, and a personal access code of a customer as an entry to said customer computer" in each of independent claims 1 and 10 renders the claims indefinite because it is unclear what claimed elements are required to enter the customer computer. Final Act. 8; Adv. Act. 2; Ans. 4. Appellants contend that one of ordinary skill in the art would understand that the claimed invention requires both a computer system identifier and one of a customer's private key, password, and personal access code to enter the customer computer. Br. 10. We agree with Appellants. The limitation recites "computer system identifier of said customer computer, ***and*** one of a private key, a password, and a personal access code of a customer" (Br., Claims App. (emphasis added)) such that a person of ordinary skill in the art

would understand that the claimed invention requires both a computer system identifier and one of a customer's private key, password, and personal access code as an entry to a customer's computer to access the encrypted information stored there. We, therefore, do not sustain the Examiner's rejection of independent claims 1 and 10 and claims 5, 8, 9, 13, 17, 28, and 29 under 35 U.S.C. § 112, second paragraph.

Claims 6, 7, 14–16, and 24–26

The Examiner determines the limitations regarding encrypting "a plurality of said customer code as customer codes" render these claims indefinite. Final Act. 8–9; Adv. Act. 2; Ans. 4–5. According to the Examiner, these limitations are unclear because the customer code is a product of encrypting customer information, not customer code. Final Act. 9.

Appellants argue that the claims are definite because they merely recite a plurality of the customer code previously recited in the respective independent claim. Br. 10. Appellants' argument is not persuasive.

Each of the independent claims 1, 10, and 18 recites encrypting ***customer information*** as a customer code, yet these dependent claims recite encrypting a plurality of the ***customer code*** as customer codes. Br., Claims App. Consequently, it is unclear whether the term "customer codes" refers to a plurality of encrypted customer information or an encrypted plurality of customer code. As such, we sustain the rejection of claims 6, 7, 14–16, and 24–26 under 35 U.S.C. § 112, second paragraph.

Claim 21

The Examiner determines claim 21 is indefinite because it is unclear whether the recited financial institution is part of the claimed system. Final

Act. 10; Ans. 5–6. Appellants contend that the claim is not indefinite because it explains the actions of others with which the claimed system operates. Br. 11. We agree with Appellants.

Claim 21 depends from independent claim 18, which is directed to a system comprising a non-transitory storage device storing instructions executable by a processor of a customer computer. Br., Claims App. A person of ordinary skill would appreciate that a financial institution is not part of a non-transitory storage device having instructions that are executable by a customer's computer. Accordingly, we do not sustain the rejection of claim 21 under 35 U.S.C. § 112, second paragraph.

Claim 23

The Examiner determines claim 23 is indefinite because the term "site" suggests a location or place, which is not commensurate with a system claim. Final Act. 10; Ans. 7. Appellants argue that a person of ordinary skill in the art would understand that the term "site" can be a network location, as described in the Specification.

Like claim 21, claim 23 also depends from independent claim 18, which, as described above, is directed to a system comprising a non-transitory storage device. Br., Claims App. Regardless of whether the term "site" is a physical location or a network location, a person of ordinary skill in the art would appreciate that the claimed site is not part of a non-transitory storage device. Accordingly, we do not sustain the rejection of claim 23 under 35 U.S.C. § 112, second paragraph.

Obviousness

The Examiner relies on the combined teachings of Flitcroft, Schenkler, Shmueli, and Mi to render obvious the claimed invention. In particular, the Examiner finds that Flitcroft teaches encrypting customer information as a customer code on a storage device on a customer computer (Final Act. 13), and that Mi teaches multi-factor authentication, i.e., requiring a password and a computer system identifier, to access encrypted information (Final Act. 15). Appellants have not persuaded us that the Examiner erred in determining that the claimed invention set forth in independent claims 1, 10, and 18 would have been obvious. Br. 15–18.

In particular, we disagree with Appellants that Flitcroft teaches away from encryption systems. Br. 15. Although Appellants are correct that Flitcroft discloses single use credit cards to prevent fraud, Flitcroft teaches that these credit card numbers are encrypted. Flitcroft ¶¶ 72, 120; Final Act. 16; Ans. 8. Given that encryption is part of Flitcroft's system, we fail to see how Flitcroft teaches away from using encryption. *See In re Haruna*, 249 F.3d 1327, 1335 (Fed. Cir. 2001) ("A reference may be said to teach away when a person of ordinary skill, upon reading the reference would be led in a direction divergent from the path that was taken by the applicant.")

We also disagree with Appellants that the Examiner's proposed combination would not result in the claimed invention, which requires two pieces of information, namely a computer system identifier and one of a customer's private key, password, and personal access code, to access the encrypted information, i.e., customer code. Br. 15–18. Specifically, Appellants contend that a person of ordinary skill would not have been

motivated to require two pieces of information to access the customer code on the customer's computer because Mi uses two-factor validation only to determine whether a user is accessing a server from an unknown computer. *Id.* at 17.

Mi teaches that "[w]hen two factors are required, an unauthorized user who obtains only an authorized user's ID/password may be denied access when trying to establish a connection from a different platform." Mi 11:16–19. We agree with the Examiner that a person of ordinary skill in the art would appreciate Mi's teaching of two-factor validation would similarly improve the security of Flitcroft's system by providing a heightened requirement for access to the customer code stored on a customer's computer. Ans. 9; *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007) ("[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.").

In view of the foregoing, we sustain the rejection of independent claims 1, 10, and 18 under 35 U.S.C. § 103(a). Appellants do not present separate argument for dependent claims 5–9, 13–17, 21, and 23–30, and we sustain the rejection of these claims for the same reasons as the independent claims.

DECISION

The Examiner's decision to reject claims 1, 5–10, 13–17, 28, and 29 under 35 U.S.C. § 112, first paragraph, is affirmed.

The Examiner's decision to reject claims 1, 5, 8–10, 13, 17, 21, 23, 28, and 29 under 35 U.S.C. § 112, second paragraph, is reversed.

The Examiner decision to reject claims 6, 7, 14–16, and 24–26 under 35 U.S.C. § 112, second paragraph, is affirmed.

The Examiner's decision to reject claims 1, 5–10, 13–18, 21, and 23–30 under 35 U.S.C. § 103(a) is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED